日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 Date of Application:	２００４年　６月１４日
出 願 番 号 Application Number:	特願２００４－１７５５２４
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００４－１７５５２４
出 願 人 Applicant(s):	ソニー株式会社

２００５年　７月　６日

特許庁長官
Commissioner,
Japan Patent Office

小 川

【書類名】　特許願
【整理番号】　0490010302
【提出日】　平成16年 6月14日
【あて先】　特許庁長官殿
【国際特許分類】　G06K 17/00
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　栗田　太郎
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100093241
　【弁理士】
　【氏名又は名称】　宮田　正昭
【選任した代理人】
　【識別番号】　100101801
　【弁理士】
　【氏名又は名称】　山田　英治
　【電話番号】　03-5541-7577
　【連絡先】　担当者
【選任した代理人】
　【識別番号】　100086531
　【弁理士】
　【氏名又は名称】　澤田　俊夫
【手数料の表示】
　【予納台帳番号】　048747
　【納付金額】　16,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9904833

【書類名】特許請求の範囲
【請求項１】
メモリ空間に配置されたファイルを管理する情報管理装置であって、
バックアップする１以上のファイルについてのアーカイブ・ファイルを、該アーカイブ・ファイルの展開先の識別情報を付して作成するアーカイブ・ファイル作成手段を備える、
ことを特徴とする情報管理装置。
【請求項２】
アーカイブ・ファイルを作成したファイルへのアクセスを管理するアクセス管理手段をさらに備える、
ことを特徴とする請求項１に記載の情報管理装置。
【請求項３】
同時にオープンすべきファイルを連携指定するファイル連携指定手段をさらに備え、
アーカイブ・ファイルを作成したファイルと、該ファイルへのアクセス管理情報を記述したアクセス管理情報ファイルとを前記ファイル連携指定手段により連携指定し、
前記アクセス管理手段は、アーカイブ・ファイルを作成したファイルへのアクセスが行なわれた際に、アクセス管理情報ファイルを同時にオープンし、アクセス管理情報に基づいてアクセス管理を行なうとともに、アクセス管理情報の内容を更新する、
ことを特徴とする請求項２に記載の情報管理装置。
【請求項４】
前記アクセス管理情報ファイルは、アクセス管理情報としてアーカイブ・ファイルを作成したファイルへのカウンタ値を記述し、
前記アクセス管理手段は、アクセス管理情報ファイルをオープンする度にカウンタ値をデクリメントする、
ことを特徴とする請求項３に記載の情報管理装置。
【請求項５】
前記メモリ空間ではディレクトリ構造が採用され、
前記アーカイブ・ファイル作成手段は、バックアップするディレクトリについてのアーカイブ・ファイルを、該アーカイブ・ファイルの展開先の識別情報を付して作成する、
ことを特徴とする請求項１に記載の情報管理装置。
【請求項６】
メモリ空間に配置されたファイルを管理する情報管理方法であって、
バックアップする１以上のファイルについてのアーカイブ・ファイルを、該アーカイブ・ファイルの展開先の識別情報を付して作成するアーカイブ・ファイル作成ステップを備える、
ことを特徴とする情報管理方法。
【請求項７】
アーカイブ・ファイルを作成したファイルへのアクセスを管理するアクセス管理ステップをさらに備える、
ことを特徴とする請求項６に記載の情報管理方法。
【請求項８】
同時にオープンすべきファイルを連携指定するファイル連携指定ステップをさらに備え、
アーカイブ・ファイルを作成したファイルと、該ファイルへのアクセス管理情報を記述したアクセス管理情報ファイルとを前記ファイル連携指定ステップにより連携指定し、
前記アクセス管理ステップでは、アーカイブ・ファイルを作成したファイルへのアクセスが行なわれた際に、アクセス管理情報ファイルを同時にオープンし、アクセス管理情報に基づいてアクセス管理を行なうとともに、アクセス管理情報の内容を更新する、
ことを特徴とする請求項７に記載の情報管理方法。
【請求項９】

前記アクセス管理情報ファイルは、アクセス管理情報としてアーカイブ・ファイルを作成したファイルへのカウンタ値を記述し、
前記アクセス管理ステップでは、アクセス管理情報ファイルをオープンする度にカウンタ値をデクリメントする、
ことを特徴とする請求項８に記載の情報管理方法。
【請求項１０】
前記メモリ空間ではディレクトリ構造が採用され、
前記アーカイブ・ファイル作成ステップでは、バックアップするディレクトリについてのアーカイブ・ファイルを、該アーカイブ・ファイルの展開先の識別情報を付して作成する、
ことを特徴とする請求項６に記載の情報管理方法。

【書類名】明細書
【発明の名称】情報管理装置及び情報管理方法

【技術分野】
【０００１】
本発明は、比較的大容量のメモリ領域に格納された情報へのアクセスを管理する情報管理装置及び情報管理方法に係り、特に、メモリ領域上に電子的な価値情報を格納して電子決済を始めとするセキュアな情報のやり取りを行なう情報管理装置及び情報管理方法に関する。
【０００２】
さらに詳しくは、本発明は、メモリ領域上にさまざまなファイルを割り当てて、サービス運用のための情報を管理する情報管理装置及び情報管理方法に係り、特に、メモリ領域上に電子的に格納されている価値情報のコピー若しくはバックアップを行ない、端末間での価値情報の移動を円滑に行なう情報管理装置及び情報管理方法に関する。
【背景技術】
【０００３】
ＩＣカードに代表される非接触・近接通信システムは、操作上の手軽さから、広範に普及している。ＩＣカードの一般的な使用方法は、利用者がＩＣカードをカード・リーダ／ライタをかざすことによって行なわれる。カード・リーダ／ライタ側では常にＩＣカードをポーリングしており外部のＩＣカードを発見することにより、両者間の通信動作が開始する。例えば、暗証コードやその他の個人認証情報、電子チケットなどの価値情報などをＩＣカードに格納しておくことにより、キャッシュ・ディスペンサやコンサート会場の出入口、駅の改札口などにおいて、入場者や乗車者の認証処理を行なうことができる。
【０００４】
最近では、微細化技術の向上とも相俟って、比較的大容量のメモリを持つＩＣカードが出現している。大容量メモリ付きのＩＣカードによれば、メモリ空間上にファイル・システムを展開し、複数のアプリケーションを同時に格納しておくことにより、１枚のＩＣカードを複数の用途に利用することができる。例えば、１枚のＩＣカード上に、電子決済を行なうための電子マネーや、特定のコンサート会場に入場するための電子チケットなど、複数のアプリケーションを格納しておくことにより、１枚のＩＣカードをさまざまな用途に適用させることができる。ここで言う電子マネーや電子チケットは、利用者が提供する資金に応じて発行される電子データを通じて決済（電子決済）される仕組み、又はこのような電子データ自体を指す。
【０００５】
また、ＩＣカードやカード用リーダ／ライタ（カード読み書き装置）が無線・非接触インターフェースの他に、外部機器と接続するための有線インターフェースを備え、携帯電話機、ＰＤＡ（Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｃｅ）やＣＥ（Ｃｏｎｓｕｍｅｒ Ｅｌｅｃｔｒｏｎｉｃｓ）機器、パーソナル・コンピュータなどの各機器に内蔵して用いることにより，これらの機器にＩＣカード及びカード・リーダ／ライタのいずれか一方又は双方の機能を装備することができる。このような場合、ＩＣカード技術を汎用性のある双方向の近接通信インターフェースとして利用することができる。
【０００６】
例えば、コンピュータや情報家電機器のような機器同士で近接通信システムが構成される場合には、ＩＣカードを利用した非接触通信は一対一で行なわれる。また、ある機器が非接触ＩＣカードのような機器以外の相手デバイスと通信することも可能であり、この場合においては、１つの機器と複数のカードにおける一対多の通信を行なうアプリケーションも考えられる。
【０００７】
また、電子決済を始めとする外部との電子的な価値情報のやり取りなど、ＩＣカードを利用したさまざまなアプリケーションを、情報処理端末上で実行することができる。例えば、情報処理端末上のキーボードやディスプレイなどのユーザ・インターフェースを用い

ＩＣカードに対するユーザ・インタフェースを情報処理端末上で行なうことができる。また、ＩＣカードが携帯電話機と接続されていることにより、ＩＣカード内に記憶された内容を電話網経由でやり取りすることもできる。さらに、携帯電話機からインターネット接続して利用代金をＩＣカードで支払うことができる。

【０００８】

あるサービス提供元事業者用のファイル・システムをＩＣカードの内蔵メモリに割り当てて、このファイル・システム内で当該事業者によるサービス運用のための情報（例えば、ユーザの識別・認証情報や残りの価値情報、使用履歴（ログ）など）を管理することにより、従来のプリペイド・カードや店舗毎のサービス・カードに置き換わる、非接触・近接通信を基調とした有用なサービスを実現することができる。

【０００９】

従来、サービス提供元事業者毎にＩＣカードが個別に発行され、ユーザの利用に供されていた。このため、ユーザは、利用したいサービス毎にＩＣカードを取り揃え、携帯しなければならなかった。これに対し、比較的大容量のメモリ空間を持つＩＣカードによれば、単一のＩＣカードの内蔵メモリに複数のサービスに関する情報を記録するだけの十分な容量を確保することができる（例えば、非特許文献１を参照のこと）。

【００１０】

ＩＣカード内のメモリ領域は、初期状態ではＩＣカード発行者がメモリ領域全体を管理しているが、ＩＣカード発行者以外のサービス提供元事業者がメモリ領域から新たなファイル・システムを分割し、それぞれのサービス運用を実現するためのアプリケーションに割り当てる。ファイル・システムの分割は、仮想的なＩＣカードの発行である。また、メモリ領域の分割操作を繰り返すことにより、ＩＣカード内のメモリ領域は複数のファイル・システムが共存する構造となり、１枚のＩＣカードでマルチアプリケーションすなわち多種多様なアプリケーションを提供することができる。

【００１１】

【非特許文献１】「無線ＩＣタグのすべて　ゴマ粒チップでビジネスが変わる」（１０６～１０７頁、ＲＦＩＤテクノロジ編集部、日経ＢＰ社、２００４年４月２０日発行）

【発明の開示】

【発明が解決しようとする課題】

【００１２】

上述したように、ＩＣカード若しくはＩＣチップ上には、電子マネーや電子チケットといったさまざまな価値情報を安全に格納することができる。利用者の利便性を考慮すると、ＩＣカードに担持されているデータのバックアップをとることが必要となってくる。価値情報を格納したＩＣチップを内蔵した携帯電話機を機種変更する場合や、ＩＣチップを搭載したカードや機器に障害が発生した場合などである。

【００１３】

ところが、ＩＣカード内のデータのコピー若しくはバックアップをとる際には、２重化を防止しなければならない。現金の移動であれば、財布から財布へ移動することはあっても、増えることはない。これに対し、電子マネーや電子チケットなどの価値情報は、現金相当の価値を有するものの、その実体はデジタル・データなので、データ移動元のＩＣカードとデータ移動先のＩＣカードの双方に元の価値情報が２重化して存在してしまい、双方で価値情報が利用可能になる可能性がある。

【００１４】

また、ＩＣカード内のデータのコピー若しくはバックアップをとる際、正しい相手に移動しなければならない。この際、ＩＣカードがマルチアプリケーション、すなわち複数のサービス提供元事業者の管理下にまたがっている場合には、手続が煩雑となる。

【００１５】

例えば、携帯電話機の機種変更手続に併せて、ＩＣチップ内の価値情報を移動することも考えられる。しかしながら、移動途中における通信障害やマシン障害などによる価値情

報の消失や、価値情報の不正な複製や改竄が行われる可能性があり、電話会社にとっては責任が過大である。

【００１６】

一方、ＩＣチップ内の各価値情報の移動をそれぞれのサービス提供元事業者によって行なうという方法も考えられる。この方法は責任分離という観点からは有効であるが、ユーザは携帯端末の機種変更に伴い、複数の手続を取らなければならなくなる。

【００１７】

本発明は上述したような技術的課題を鑑みたものであり、その主な目的は、メモリ領域上にさまざまなファイルを割り当てて、サービス運用のための情報を管理することができる、優れた情報管理装置及び情報管理方法を提供することにある。

【００１８】

本発明のさらなる目的は、メモリ領域上に電子的に格納されている価値情報のコピー若しくはバックアップを行ない、端末間での価値情報の移動を円滑に行なうことができる、優れた情報管理装置及び情報管理方法を提供することにある。

【課題を解決するための手段】

【００１９】

本発明は、上記課題を参酌してなされたものであり、メモリ空間に配置されたファイルを管理する情報管理装置であって、

バックアップする１以上のファイルについてのアーカイブ・ファイルを、該アーカイブ・ファイルの展開先の識別情報を付して作成するアーカイブ・ファイル作成手段を備える、

ことを特徴とする情報管理装置である。

【００２０】

ここで言う情報管理装置は、無線通信部及び、データ送受信機能とデータ処理部を有するＩＣチップを内蔵する非接触ＩＣカード、表面に端子を有する接触ＩＣカード、接触／非接触ＩＣカードと同様の機能を有するＩＣチップを携帯電話機、ＰＨＳ（Ｐｅｒｓｏｎａｌ Ｈａｎｄｙｐｈｏｎｅ Ｓｙｓｔｅｍ）、ＰＤＡ（Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｃｅ）などの情報通信端末装置に内蔵した装置である。以下では、これらを総称して、単に「ＩＣカード」と呼ぶこともある。

【００２１】

この情報管理装置は、ＥＥＰＲＯＭなどのデータ蓄積メモリを含むメモリ領域とデータ処理部を有するとともに、データ通信機能を有するものである。携帯電話機などの場合は、ＩＣチップを内蔵するＩＣカードなどの外部記憶媒体を着脱可能に構成してもよい。また、携帯電話会社が発行する契約者情報を記録したＳＩＭ（Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｙ Ｍｏｄｕｌｅ）機能をＩＣチップに搭載してもよい。情報管理装置は、インターネットなどの情報通信ネットワークを介してデータ通信を行なってもよいし、外部端末装置と有線又は無線で直接データ通信を行なってもよい。

【００２２】

本発明は、ＩＣカードが持つ耐タンパ性と認証機能を利用した、価値情報のやり取りなどを含んだセキュリティが要求されるサービスの提供に関するするものである。ＩＣカード内のメモリは、一般に、複数のエリアに分割され、エリア毎に異なる暗号鍵を設けてアクセスの制御が行なわれる。ここで言うエリアは、メモリ空間を分割して得られるファイル・システム、若しくはファイル・システム内のディレクトリや個別のファイルに相当する。

【００２３】

ここで、利用者の利便性を考慮すると、ＩＣカードに担持されているデータのバックアップをとることが必要となってくるが、特にマルチアプリケーション用途のＩＣカードでは、その処理が煩雑になるという問題がある。

【００２４】

これに対し、本発明では、ＩＣカード内のデータから移動先の端末ＩＤを含めたアーカ

ライブラリファイルを作成し、所定の保管場所に保管するので、価値情報を安全にバックアップすることができる。また、アーカイブ・ファイルは、端末ＩＤで指定された機器でしか展開できないようにする。

【００２５】

また、ＩＣカード内のファイルやディレクトリへのアクセスをカウンタで管理する仕組みを導入し、アーカイブ・ファイルを保管場所にアーカイブした後は元のファイルのカウンタ値を消滅させてアクセスできないようにすることで、ファイルの移動を実現することができる。

【００２６】

情報管理装置は、同時にオープンすべきファイルを連携指定するファイル連携指定手段をさらに備え、アーカイブ・ファイルを作成したファイルと、該ファイルへのアクセス管理情報を記述したアクセス管理情報ファイルとを前記ファイル連携指定手段により連携指定する。そして、前記アクセス管理手段は、アーカイブ・ファイルを作成したファイルへのアクセスが行なわれた際に、アクセス管理情報ファイルを同時にオープンし、アクセス管理情報に基づいてアクセス管理を行なうとともに、アクセス管理情報の内容を更新するようにする。ここで、前記アクセス管理情報ファイルは、アクセス管理情報としてアーカイブ・ファイルを作成したファイルへのカウンタ値を記述しており、前記アクセス管理手段は、アクセス管理情報ファイルをオープンする度にカウンタ値をデクリメントする。

【発明の効果】

【００２７】

本発明によれば、メモリ領域上にさまざまなファイルを割り当てて、サービス運用のための情報を管理することができる、優れた情報管理装置及び情報管理方法を提供することができる。

【００２８】

また、本発明によれば、メモリ領域上に電子的に格納されている価値情報のコピー若しくはバックアップを行ない、端末間での価値情報の移動を円滑に行なうことができる、優れた情報管理装置及び情報管理方法を提供することができる。

【００２９】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【発明を実施するための最良の形態】

【００３０】

以下、図面を参照しながら本発明の実施形態について詳解する。

【００３１】

<u>Ａ．ＩＣカードによる非接触データ通信システム</u>

図１には、本発明を適用可能な非接触ＩＣカード通信システムの構成を模式的に示している。

【００３２】

この非接触カードシステムは、カード・リーダ／ライタ１と、ＩＣカード２と、コントローラ３で構成され、カード・リーダ／ライタ１とＩＣカード２との間では、電磁波を利用して非接触で、データの送受信が行なわれる。すなわち、カード・リーダ／ライタ１がＩＣカード２に所定のコマンドを送信し、ＩＣカード２は受信したコマンドに対応する処理を行なう。そして、ＩＣカード２は、その処理結果に対応する応答データをカード・リーダ／ライタ１に送信する。

【００３３】

カード・リーダ／ライタ１は、所定のインターフェース（例えば、ＲＳ－４８５Ａの規格などに準拠したもの）を介してコントローラ３に接続されている。コントローラ３は、カード・リーダ／ライタ１に対し制御信号を供給することで、所定の処理を行なわせる。

【００３４】

<u>Ｂ．ＩＣカードの運用</u>

図２には、ＩＣカードを用いて実現される、電子マネーや電子クラブ、その他の価値情報を運用するサービス提供システムの全体的構成を模式的に示している。

【００３５】

図示のシステム１００は、例えば、ＩＣカード発行者１２１が使用する発行者用通信装置１１１と、カード記憶領域運用者１２２が使用する運用者用通信装置１１２と、装置製造者１２３が使用する製造者用通信装置１１３と、カード記憶領域使用者１２４が使用する記憶領域分割装置１１４及び運用ファイル登録装置１１５とで構成される。

【００３６】

ＩＣカード発行者１２１がカード所有者１２６にＩＣカード１１６を発行した場合に、所定の条件に基づいて、カード記憶領域使用者１２４によって提供されるサービスに係わるファイル・データをＩＣカード１６に登録し、カード所有者１２６が単体のＩＣカード１１６を用いて、ＩＣカード発行者１２１及びカード記憶領域使用者１２４の双方のサービスを受けることを可能にするものである。

【００３７】

図２に示すように、システム１００では、発行者用通信装置１１１、運用者用通信装置１１２、製造者用通信装置１１３、記憶領域分割装置１１４及び運用ファイル登録装置１１５が、ネットワーク１１７を介して接続される。

【００３８】

ＩＣカード発行者１２１は、ＩＣカード１１６の発行を行なう者であり、ＩＣカード１１６を用いて自らのサービスを提供する。

【００３９】

カード記憶領域運用者１２２は、ＩＣカード発行者１２１からの依頼を受けて、ＩＣカード発行者１２１が発行したＩＣカード１１６内の記憶部（半導体メモリ）に構成される記憶領域のうち、ＩＣカード発行者１２１が使用しない記憶領域をカード記憶領域使用者１２４に貸し出すサービスを行なう者である。

【００４０】

装置製造者１２３は、カード記憶領域運用者１２２から依頼を受けて、記憶領域分割装置１１４を製造し、カード記憶領域使用者１２４に納品する者である。

【００４１】

カード記憶領域使用者１２４は、カード記憶領域運用者１２２に依頼を行ない、ＩＣカード１１６の記憶領域を使用して自らの独自のサービスを提供する者であり、メモリ領域を分割して新たなファイル・システムを作成するサービス提供元事業者に相当し、自己のファイル・システムを利用して自身のサービス提供を行なう。

【００４２】

カード所有者１２６は、ＩＣカード発行者１２１からＩＣカード１１６の発行を受け、ＩＣカード発行者１２１が提供するサービスを受ける者すなわちエンドユーザである。カード所有者１２６は、ＩＣカード１１６の発行後に、カード記憶領域使用者１２４が提供するサービスを受けることを希望する場合には、記憶領域分割装置１１４及び運用ファイル登録装置１１５を用いて、カード記憶領域使用者１２４のサービスに係わるファイル・データをＩＣカード１１６に記憶し、その後、カード記憶領域使用者１２４のサービスを受けることができるようになる。

【００４３】

システム１００は、ＩＣカード発行者１２１のサービスと、カード記憶領域使用者１２４のサービスとを単体のＩＣカード１１６を用いて提供するに当たって、ＩＣカード発行者１２１及びカード記憶領域使用者１２４のサービスに係わるファイル・データが記憶される記憶領域に、権限を有しない他人によって不正にデータの書き込み及び書き換えなどが行なわれることを困難にする構成を有している。

【００４４】

ＩＣカード１１６は、その字義通り、カード型のデータ通信装置であってもよいし、いわゆるＩＣカード機能が実装された半導体チップを内蔵した携帯電話機（あるいはその他

の携帯端末やＰＣ機器）として具現化されることもある。

【００４５】

なお、図２では、それぞれ単数のＩＣカード発行者１２１、カード記憶領域使用者１２４及びカード所有者１２６がある場合を例示したが、これらは、それぞれ複数であってもよい。

【００４６】

Ｃ．ファイル・システム

ＩＣカードが持つ耐タンパ性と認証機能を利用して、価値情報のやり取りなどを含んだセキュリティが要求されるサービスを提供することができる。さらに本実施形態では、単一のメモリ領域上にサービス提供元事業者毎のファイル・システムを割り当て、単一のＩＣカードを複数の事業者で共有し、単一のＩＣカードにより複数のサービスを提供するようにした。

【００４７】

ＩＣカード内のメモリ領域は、初期状態では、ＩＣカード発行者がメモリ領域全体を管理している。ＩＣカード発行者以外のサービス提供元事業者がメモリ領域から新たなファイル・システムを分割するに際しては、メモリ領域の分割権限と、ＩＣカード発行者に対する認証の双方が要求される。

【００４８】

メモリ領域が一旦分割されると、ファイル・システムへのアクセスは、元のＩＣカードの発行者ではなく、ファイル・システム自体のサービス提供元事業者への認証が要求される。したがって、ファイル・システム間の境界がファイヤ・ウォールとして機能し、他のファイル・システムからの不正なアクセスを好適に排除することができる。また、ユーザにとっては、各サービス利用時において事業者自らが発行したＩＣカードであるかのような使い勝手を確保することができる。そして、メモリ領域の分割操作を繰り返すことにより、ＩＣカード内のメモリ領域は複数のファイル・システムが共存する構造となる。ファイル・システムの分割は、仮想的なＩＣカードの発行である。

【００４９】

ここで、図３～図６を参照しながら、ＩＣカード内のメモリ領域の運用形態について説明する。

【００５０】

図３には、元のカード発行者が自らのファイル・システムのみを管理しているメモリ領域の状態を示している。元のカード発行者のシステム・コードＳＣ１は、システム・コードの管理機構が付与する。外部機器又はプログラムがカード発行者のファイル・システムにアクセスする場合は、ＳＣ１を識別コード（すなわち、要求コマンドの引数）とする。

【００５１】

図４には、カード発行者が自らのファイル・システムの空き領域の内で、ある範囲のメモリを領域管理者に貸与（又は譲渡）することが許可できることを示している。この段階では，まだメモリ領域上のファイル・システムに対して分割が行なわれている訳ではない。カード発行者は、自らのファイル・システムに空き領域はあるうちは、複数の領域管理者に対して、メモリを貸与することを許可できる。例えば、４ビットのシステム・コードでファイル・システムを識別するという実装では、最大１６分割（１５回まで分割）することができる。

【００５２】

図５には、他のサービス提供元事業者が、カード発行者から許可された領域においてメモリ領域を分割し、新たなファイル・システムを生成した状態を示している。この新規ファイル・システムには、システム・コードの管理機構からシステム・コードＳＣ２が付与されている。外部機器又はプログラムが、当該メモリ領域管理者（サービス提供元事業者）の運用するファイル・システムにアクセスする場合は、ＳＣ２を識別コード（要求コマンドの引数）とする。

【００５３】

図６には、共通領域管理者が、カード発行者から許可された領域において、共通領域のシステム・コードＳＣ０でメモリを分割した状態を示している。外部機器又はプログラムがこの共通領域管理者の運用領域であるファイル・システムにアクセスする場合には、そのシステム・コードＳＣ０を識別コード（要求コマンドの引数）とする。

【００５４】

ＩＣカードのメモリ領域は、分割操作を繰り返すことにより、図７に示すように複数のファイル・システムが共存する構造となる。元のカード発行者、並びにカード発行者の許可によりＩＣカード上で自己のファイル・システムを取得したサービス提供元事業者は、それぞれ自己のファイル・システムを利用して、エリアやサービスを配設し、自身の事業展開に利用することができる。

【００５５】

ここで、１つのファイル・システム内での運用形態について説明する。基本的には、どのファイル・システムにおいても同様の動作が実現されるものとする。

【００５６】

ファイル・システム内には、電子決済を始めとする外部との電子的な価値情報のやり取りなどのアプリケーションを実現するための、１以上のファイルが配置されている。アプリケーションに割り当てられているメモリ領域を「サービス・メモリ領域」と呼ぶ。また、アプリケーションの利用、すなわち該当するサービス・メモリ領域へアクセスする処理動作のことを「サービス」と呼ぶ。サービスには、メモリへの読み出しアクセス、書き込みアクセス、あるいは電子マネーなどの価値情報に対する価値の加算や減算などが挙げられる。

【００５７】

ユーザがアクセス権を持つかどうかに応じてアプリケーションの利用すなわちサービスの起動を制限するために、アプリケーションに対して暗証コードすなわちＰＩＮを割り当て、サービス実行時にＰＩＮの照合処理を行なうようになっている。また、サービス・メモリ領域へのアクセスは、アプリケーションのセキュリティ・レベルなどに応じて、適宜暗号化通信が行なわれる。

【００５８】

本実施形態では、ＩＣカード内のメモリ領域に設定されているそれぞれのファイル・システムに対して、「ディレクトリ」に類似する階層構造を導入する。そして、メモリ領域に割り当てられた各アプリケーションを、所望の階層の「エリア」に登録することができる。

【００５９】

例えば、一連のトランザクションに使用される複数のアプリケーション、あるいは関連性の深いアプリケーション同士を同じエリア内のサービス・メモリ領域として登録する（さらには、関連性の深いエリア同士を同じ親エリアに登録する）ことによって、メモリ領域のアプリケーションやエリアの配置が整然とし、ユーザにとってはアプリケーションの分類・整理が効率化する。

【００６０】

また、ファイル・システムへのアクセス権を階層的に制御するために、アプリケーション毎にＰＩＮを設定できる以外に、各エリアに対してもＰＩＮを設定することができるようにしている。例えば、あるエリアに該当するＰＩＮを入力することにより、照合処理並びに相互認証処理を経て、エリア内のすべてのアプリケーション（並びにサブエリア）へのアクセス権を与えるようにすることもできる。したがって、該当するエリアに対するＰＩＮの入力を１回行なうだけで、一連のトランザクションで使用されるすべてのアプリケーションのアクセス権を得ることができるので、アクセス制御が効率化するとともに、機器の使い勝手が向上する。

【００６１】

さらに、あるサービス・メモリ領域に対するアクセス権限が単一でないことを許容し、それぞれのアクセス権限毎、すなわちサービス・メモリ領域において実行するサービスの

内容毎に、暗証コードを設定することができる。例えば、同じサービス・メモリ領域に対して起動するサービスが「読み出し」と「読み出し及び書き込み」とでは、別々のＰＩＮが設定される。また、電子マネーやその他の価値情報に対する「増額」と「減額」とでは、別々のＰＩＮが設定される。また、あるメモリ領域に対する読み出しについてはＰＩＮの入力が必要でないが、書き込む場合にはＰＩＮの入力を必須とさせることが可能である。

【００６２】

図８には、ファイル・システム内のデータ構造例を模式的に示している。図示の例では、ファイル・システムが持つ記憶空間には、「ディレクトリ」に類似する階層構造が導入されている。すなわち、メモリ領域に割り当てられた各アプリケーションを、所望の階層エリアにサービス・メモリ領域として登録することができる。例えば、一連のトランザクションに使用されるアプリケーションなど、関連性の深いアプリケーション同士を同じエリアに登録する（さらには、関連性の深いエリア同士を同じ親エリアに登録する）ことができる。

【００６３】

また、ファイル・システム内に割り当てられたアプリケーション（すなわちサービス・メモリ領域）並びにエリアは暗証コード定義ブロックを備えている。したがって、アプリケーション毎に、あるいはエリア毎にＰＩＮを設定することができる。また、ファイル・システムに対するアクセス権は、アプリケーション単位で行なうとともに、並びにエリア単位で行なうことができる。

【００６４】

さらに、あるサービス・メモリ領域に対するアクセス権限が単一でなく、実行するサービスの内容毎に、ＰＩＮを設定することができる。例えば、同じサービス・メモリ領域に対して起動するサービスが「読み出し」と「読み出し及び書き込み」とでは、別々のＰＩＮが設定され、また、電子マネーやその他の価値情報に対する「増額」と「減額」とでは、別々のＰＩＮが設定される。

【００６５】

照合部は、例えばＩＣカードを利用した非接触データ通信などのプロトコル・インターフェースを介して送られてくるＰＩＮを、各アプリケーション又はディレクトリに割り当てられたエリア又はサービス・メモリ領域に設定されている暗証コードと照合して、一致するメモリ領域に対するアクセスを許可する。アクセスが許可されたメモリ領域は、プロトコル・インターフェースを介して読み書きが可能となる。

【００６６】

図９には、ファイル・システムの基本構成を示している。図８を参照しながら既に説明したように、ファイル・システムに対して、「ディレクトリ」に類似する階層構造が導入され、所望の階層のエリアに、アプリケーションに割り当てられたサービス・メモリ領域を登録することができる。図９に示す例では、エリア００００定義ブロックで定義されるエリア００００内に、１つのサービス・メモリ領域が登録されている。

【００６７】

図示のサービス・メモリ領域は、１以上のユーザ・ブロックで構成される。ユーザ・ブロックはアクセス動作が保証されているデータ最小単位のことである。このサービス・メモリ領域に対しては、サービス０１０８定義ブロックで定義されている１つのサービスすなわちサービス０１０８が適用可能である。

【００６８】

エリア単位、並びにアプリケーション単位でアクセス制限を行なう以外に、サービスの種類毎に暗証コードを設定して、サービス単位でアクセス制限を行なうことができる。アクセス制限の対象となるサービスに関する暗証コード設定情報は、暗証コード専用のサービス（すなわち「暗証コード・サービス」）として定義される。図９に示す例では、サービス０１０８に関する暗証コードが暗証コード・サービス０１２８定義ブロックとして定義されている。その暗証コード・サービスの内容は暗証コード・サービス・データ・ブロ

ンに格納されている。

【００６９】

サービス０１０８に対する暗証コード・サービスが有効になっている場合、サービス０１０８を起動してそのユーザ・ブロックに読み出し又は書き込み動作を行なう前に、暗証コード・サービス０１２８を使用した暗証コードの照合が必要となる。具体的には、暗号化あり読み書き（Ｒｅａｄ／Ｗｒｉｔｅ）コマンドを使用する場合は、相互認証前にサービス０１０８に対する暗証コードすなわちＰＩＮの照合を行なう。

【００７０】

また、アプリケーションに割り当てられたサービス・メモリ領域を所望の階層のエリアに登録するとともに、エリアを階層化する（関連性の深いエリア同士を同じ親エリアに登録する）ことができる。この場合、エリア毎にＰＩＮを設定することにより、エリアをアクセス制限の単位とすることができる。図１０には、ＩＣカードのメモリ空間においてエリアが階層化されている様子を示している。同図に示す例では、エリア０００００定義ブロックで定義されているエリア０００００内に、エリア１０００定義ブロックで定義されている別のエリア１０００が登録されている。

【００７１】

図１０に示す例では、さらにエリア１０００内には、２つのサービス・メモリ領域が登録されている。一方のサービス・メモリ領域に対しては、サービス１１０８定義ブロックで定義されているサービス１１０８と、サービス１１０Ｂ定義ブロックで定義されているサービス１１０Ｂが適用可能である。このように、１つのサービス・メモリ領域に対してサービス内容の異なる複数のサービスを定義することを、本明細書中では「オーバーラップ・サービス」と呼ぶ。オーバーラップ・サービスにおいては、同じサービス・エリアに対して、入力したＰＩＮに応じて異なるサービスが適用されることになる。また、他方のサービス・メモリ領域に対しては、サービス１１０Ｃ定義ブロックで定義されているサービス１１０Ｃが適用可能である。

【００７２】

各サービス・メモリ領域に設定されているサービスを起動してそのユーザ・ブロックに読み出し又は書き込み動作を行なうことができる。勿論、図９を参照しながら説明したように、サービス毎に暗証コード・サービスを定義することができる。この場合、サービスに対する暗証コード・サービスが有効になっているときには、暗証コード・サービスを使用したＰＩＮの照合を行なってからサービスの起動が許可される。

【００７３】

また、複数のサービスに対して共通のＰＩＮを設定したい場合には、これらサービスを含むエリアを作成し、このエリアに対して共通の暗証コード・サービスを適用することができる。

【００７４】

図１０に示す例では、エリア１０００に関する暗証コードが、暗証コード・サービス１０２０定義ブロックとして定義されている。その暗証コード・サービスの内容は暗証コード・サービス・データ・ブロックに格納されている。

【００７５】

エリア１０００に対する暗証コード・サービスが有効（後述）になっている場合、暗証コード・サービス１０２０を使用した暗証コードの照合を行なった後に、エリア１０００内の各サービスを起動してそのユーザ・ブロックに読み出し又は書き込み動作を行なうことが可能となる。

【００７６】

図１１には、内部メモリに複数のファイル・システムを設けることができるＩＣカード内のファームウェアの機能構成を模式的に示している。

【００７７】

インターフェース制御部は、非接触ＩＣカード・インターフェースによるカード・リーダ／ライタとの通信、カード・リーダ／ライタとしての通信、有線インターフェースを介

した通信、その他のＩ／Ｏインターフェースを介した通信などのプロトコル制御を行なう。

【００７８】

コマンド制御部は、インターフェース制御部を介して外部から受け取ったコマンドの処理や、外部に対するコマンド発行、コマンドの検査などを行なう。

【００７９】

セキュリティ制御部は、メモリ領域若しくはメモリ領域内の各ファイル・システムへアクセスする際の認証処理や、ファイル・システム内のディレクトリやサービスを利用する際のＰＩＮ照合などのセキュリティ処理を実現する。

【００８０】

ファイル・システム制御部は、上述したようなメモリ領域からファイル・システムへの分割（並びに分割の解消）などファイル・システム管理や、ファイル・システム内のディレクトリ構造の管理などを行なう。

【００８１】

モード管理部は、全ファイル・システム並びに個別のファイル・システムのモードの管理を行なう。ここで言うモードには、ファイル・システムの利用停止や利用再開などの状態が含まれる。

【００８２】

この他、起動制御やＲＯＭ管理、パラメータ管理、不揮発性メモリ管理、パッチ制御など、ＩＣカード内の各ハードウェア制御用のファームウェアも含まれている。

【００８３】

Ｄ．ファイルのアーカイブ

ＩＣカードに担持されているデータのバックアップをとることが必要となってくる。図１２には、ＩＣカード内のファイルやディレクトリをアーカイブするための仕組みを図解している。

【００８４】

上述したようにＩＣカード内のメモリ空間には、ディレクトリに類似する階層構造が導入されている。アーカイブ・ファイル作成部は、バックアップを取ることが指定されたファイル又はディレクトリをアーカイブするためのアーカイブ・ファイルを作成する。アーカイブ・ファイルの形式は特に限定されない。そして、アーカイブ・ファイルの展開先となる端末を識別する端末ＩＤを指定して、アーカイブ・ファイルを保管装置に格納する。これによって、ＩＣカード内のデータのバックアップが実現する。

【００８５】

保管装置は、耐タンパ性があり、格納しているアーカイブ・ファイルが外部に不正に漏洩することはない。そして、保管装置は、アーカイブ・ファイルを端末ＩＤで指定されている端末へ転送する。

【００８６】

指定された端末では、アーカイブ・ファイルを展開して元のファイルやディレクトリを復元し、利用が再開される。これによって、ＩＣカード内のデータを正しい相手に移動することができる。

【００８７】

一方、ＩＣカード内のファイルやディレクトリへのアクセスをカウンタで管理する仕組を導入し、アーカイブ・ファイルを保管場所にアーカイブした後は元のファイルのカウンタ値を消滅させてアクセスできないようにすることで、移動後のデータの２重化を防止している。

【００８８】

本実施形態では、各ファイルへのアクセス回数を管理する特殊ファイルであるカウンタ・ファイルをメモリ内若しくはディレクトリ内に配置するようにした。カウンタ・ファイルには、メモリ内若しくはディレクトリ内の各ファイルについてのアクセス回数の上限値が記載されている。

【００８９】
また、ファイル連携指定子を導入して、２以上のファイルの連携関係を設定できるようにした。ファイル連携指定子で指定されている２以上のファイルには、双方同時にオープンしなければならない、すなわち同時に認証を経なければいずれのファイルもオープンできないという制限が課される。アーカイブ・ファイルが作成されたファイルは、ファイル連携指定ファイルにより、カウンタ・ファイルと連携指定される。

【００９０】
図１３には、ファイルの連携指定したファイル・システム内の基本構成を模式的に示している。図示の例では、２以上のファイルの同時認証を指定するファイル連携指定子は、ファイル・システム内の他のファイルと同様、ファイル形式で構成されている。但し、別の形態でファイル連携指定子を定義するようにしても構わない。

【００９１】
図示の例では、ファイル・システム内には、ファイル１～３と、カウンタ・ファイルが配置されている。ファイル１～３には、ＩＣカード発行者が全カードに共通する対称鍵がそれぞれ設定されている。また、カウンタ・ファイルには個別鍵が設定されている。

【００９２】
また、図示の例では、ファイル連携指定ファイルが配置されているが、これは同時に認証できるファイルの組み合わせを指定する特殊ファイルである。ファイル連携指定ファイル自体は、他のファイルと同様に、ＩＣカード発行者がすべてのＩＣカードに共通の対称鍵で認証を行なうように設定されている。

【００９３】
ファイル連携指定ファイルは、アーカイブを行なうファイル２とカウンタ・ファイルとの連携、すなわちファイル２はカウンタ・ファイルと同時にオープンしなければならないことを規定している。

【００９４】
以下では、ファイルをオープンするときに必要な認証鍵は、ファイルに対して指定されている鍵の組合せを所定の関数ｆで演算することによって得られるものとする。

【００９５】
ファイル１は、いずれのファイル連携指定子によっても規定されていない。したがって、ファイル１自体に設定された対称鍵K_{s1}だけで相互認証を行なえば、ファイルを開くことができる。この場合の認証鍵は以下の通りとなる。

【００９６】
認証鍵K_{AUTH1}＝ｆ（ファイル１の対称鍵K_{s1}）

【００９７】
また、ファイル２は、ファイル２に設定された対称鍵で相互認証することはできず、ファイル連携指定ファイルの設定に従い、カウンタ・ファイルと同時に相互認証しなければならない。このときに利用する相互認証鍵は、ファイル２の対称鍵K_{s2}とカウンタ・ファイルの個別鍵K_pを組み合わせた結果を利用するので、個別鍵となる。

【００９８】
認証鍵K_{AUTH2}＝ｆ（ファイル２の対称鍵K_{s2}，カウンタ・ファイルの個別鍵K_p）

【００９９】
認証鍵K_{AUTH2}を以ってファイル２にアクセスした場合、カウンタ・ファイルが同時にオープンされ、カウンタ値がデクリメントされる。カウンタ値が０ｘｆｆｆｆであれば、カウンタ・ファイルはいつでも開くことができる。これに対し、カウンタ値が０であれば、カウンタ・ファイルを開くことができないため、連携指定されているファイル２もオープンすることはできない。

【０１００】
ＩＣカード内のメモリ領域に展開されるファイル・システムにディレクトリ構造を導入できる点は既に述べた通りである。この場合、ディレクトリに対しても、ファイル連携指定の仕組みを適用することができる。図１４には、ディレクトリ内のファイル、あるいは

ディレクトリとカウンタ・ファイルを連携させているファイル・システム内の構成を模式的に示している。

【０１０１】

ディレクトリ１以下では、ファイル１－１、ファイル１－２、ファイル１－３、カウンタ・ファイル１、並びにファイル連携指定ファイル１が配置されている。

【０１０２】

ファイル１－１、ファイル１－２、ファイル１－３には、ＩＣカード発行者が全カードに共通する対称鍵がそれぞれ設定されている。また、カウンタ・ファイル１には個別鍵が設定されている。また、ファイル連携指定ファイル１は、ＩＣカード発行者がすべてのＩＣカードに共通の対称鍵で認証を行なうように設定されている。

【０１０３】

ファイル連携指定ファイル１は、同時に認証できるファイルの組み合わせを指定する特殊ファイルであるが、ここでは、ファイル１－１とカウンタ・ファイル１との連携、すなわちファイル１－１はカウンタ・ファイル１と同時にオープンしなければならないことを規定している。

【０１０４】

したがって、ファイル１－２及びファイル１－３はそれぞれの対称鍵のみを用いた単独認証が可能であるのに対し、ファイル１－１は、単独認証することはできず、カウンタ・ファイル１と同時に相互認証しなければならない。このときに利用する相互認証鍵は、ファイル１－１の対称鍵K_{s1-1}と個別鍵ファイル１の個別鍵K_{p1}を組み合わせた結果を利用するので、個別鍵となる。

【０１０５】

認証鍵K_{AUTH}＝ｆ（ファイル１－１の対称鍵K_{s1-1}，カウンタ・ファイル１の個別鍵K_{p1}）

【０１０６】

ファイル１－１をオープンした場合、カウンタ・ファイル１が同時にオープンされ、カウンタ値がデクリメントされる。カウンタ値が０ｘｆｆｆｆであれば、カウンタ・ファイルはいつでも開くことができる。これに対し、カウンタ値が０であれば、カウンタ・ファイルを開くことができないため、連携指定されているファイル１－１もオープンすることはできない。

【０１０７】

一方、ディレクトリ２以下では、ファイル２－１、ファイル２－２、ファイル２－３、カウンタ・ファイル２、並びにファイル連携指定ファイル２が配置されている。

【０１０８】

ファイル２－１、ファイル２－２、ファイル２－３には、ＩＣカード発行者が全カードに共通する対称鍵がそれぞれ設定されている。また、カウンタ・ファイル２には個別鍵が設定されている。また、ファイル連携指定ファイル２は、一般ファイルと同様に、ＩＣカード発行者がすべてのＩＣカードに共通の対称鍵で認証を行なうように設定されている。

【０１０９】

ファイル連携指定ファイル２は、同時に認証できるファイルの組み合わせを指定する特殊ファイルであるが、ここでは、ディレクトリ２とカウンタ・ファイル２との連携、すなわちディレクトリ２はカウンタ・ファイル２と同時にオープンしなければならないことを規定している。

【０１１０】

したがって、ディレクトリ２以下のすべての一般ファイルは単独認証することができず、ディレクトリ２はカウンタ・ファイル２と同時に相互認証しなければならない。

【０１１１】

ディレクトリ２をオープンした場合、カウンタ・ファイル２が同時にオープンされ、カウンタ値がデクリメントされる。カウンタ値が０ｘｆｆｆｆであれば、カウンタ・ファイルはいつでも開くことができる。これに対し、カウンタ値が０であれば、カウンタ・ファ

イルを開くことができないため、連携指定されているディレクトリをもオープンすることはできない。

【０１１２】

このようにして、１以上のディレクトリ、又は１以上のファイルをアーカイブする機能を実現することができる。アーカイブするときには、以下の２つのオプションがある。これにより、ファイルのバックアップ又はコピーを実現することができる。

【０１１３】

（１）アーカイブしたデータは、アーカイブ時に指定されたＩＤを持つ端末（ファイル・システム）でしか展開することができない。

（２）アーカイブしたデータは、任意のファイル・システムにて展開することができる。

【０１１４】

例えば、ディレクトリにカウンタ・ファイルを連携させる。ディレクトリをオープンすると、カウンタ・ファイルのカウンタがデクリメントされる。ディレクトリをアーカイブする前のカウンタ値が１の場合、アーカイブ後にはカウンタが０になり、カウンタ・ファイルに認証してカウンタを書き換えない限りは、ディレクトリにアクセスすることはきない。これにより、ディレクトリやファイルの移動が実現する。

【０１１５】

ディレクトリがルート・ディレクトリの場合、ファイル・システム全体をバックアップ又はコピー又は移動することができる。

【産業上の利用可能性】

【０１１６】

以上、特定の実施形態を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。

【０１１７】

本明細書では、ＩＣカード若しくはＩＣチップに内蔵されるメモリ上に展開されたファイル空間を例にとり、ファイルを安全にアーカイブしバックアップをとる実施形態について説明してきたが、本発明の要旨はこれに限定されるものではない。例えば、ＩＣカードやＩＣチップ以外のメモリ装置上で同種のファイル・システムのアーカイブやアーカイブしたファイル・システムのアクセス管理を行なう場合に、本発明を適用し同様の作用効果を得ることができる。

【０１１８】

要するに、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈するべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【図面の簡単な説明】

【０１１９】

【図１】図１は、本発明を適用可能な非接触ＩＣカード通信システムの構成を模式的に示した図である。

【図２】図２は、ＩＣカードを用いて実現される、電子マネーや電子チケット、その他の価値情報を運用するサービス提供システムの全体的構成を模式的に示した図である。

【図３】図３は、元のカード発行者が自らのファイル・システムのみを管理しているメモリ領域の状態を示した図である。

【図４】図４は、カード発行者が自らのファイル・システムの空き領域の内で、ある範囲のメモリを領域管理者に貸与（又は譲渡）することが許可できることを示した図である。

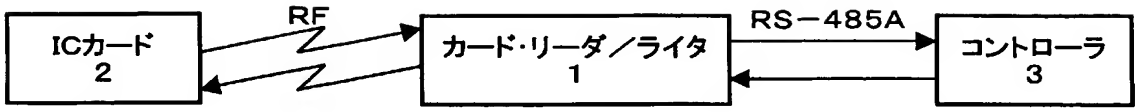
【図５】図５は、他のサービス提供元事業者が、カード発行者から許可された領域においてメモリ領域を分割し、新たなファイル・システムを生成した状態を示した図である。

【図６】図６は、共通領域管理者が、カード発行者から許可された領域において、共通領域のシステム・コードＳＣ０でメモリを分割した状態を示した図である。
【図７】図７は、ＩＣカードのメモリ領域内に複数のファイル・システムが共存する構造を示した図である。
【図８】図８は、ファイル・システム内のデータ構造例を模式的に示した図である。
【図９】図９は、ファイル・システムの基本構成を示した図である。
【図１０】図１０は、ＩＣカードのメモリ空間においてエリアが階層化されている様子を示した図である。
【図１１】図１１は、ＩＣカード内のファームウェアの機能構成を模式的に示した図である。
【図１２】図１２は、ＩＣカード内のファイルやディレクトリをアーカイブするための仕組みを示した図である。
【図１３】図１３は、ファイルの連携指定したファイル・システム内の基本構成を模式的に示し
【図１４】図１４は、ディレクトリ内のファイル、あるいはディレクトリとカウンタ・ファイルを連携させているファイル・システム内の構成を模式的に示した図である。

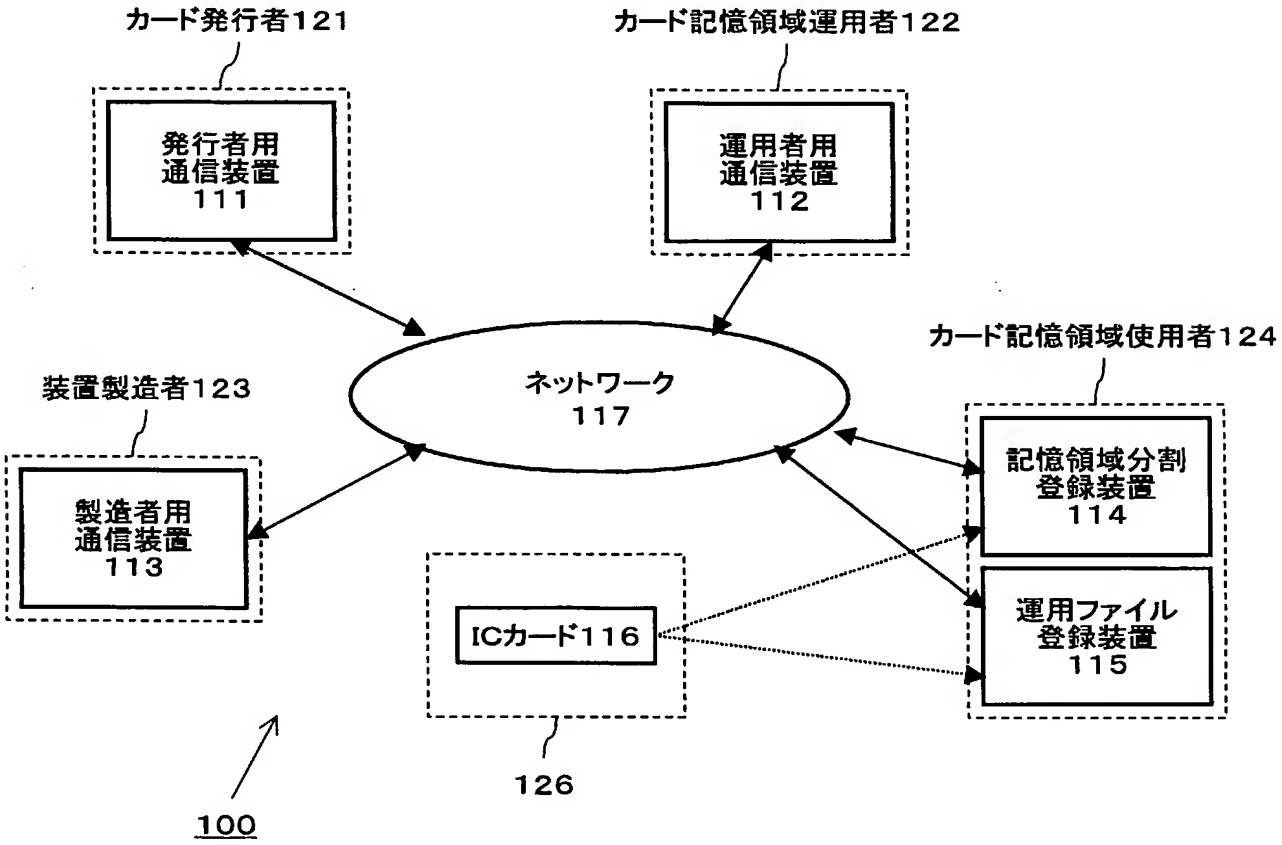
【符号の説明】
【０１２０】
１…カード・リーダ／ライタ
２…ＩＣカード
３…コントローラ
１１１…発行者用通信装置
１１２…運用者用通信装置
１１３…製造者用通信装置
１１４…記憶領域分割登録装置
１１５…運用ファイル登録装置
１１６…ＩＣカード
１１７…ネットワーク
１２１…カード発行者
１２２…カード記憶領域運用者
１２３…装置製造者
１２４…カード記憶領域使用者

【書類名】 図面

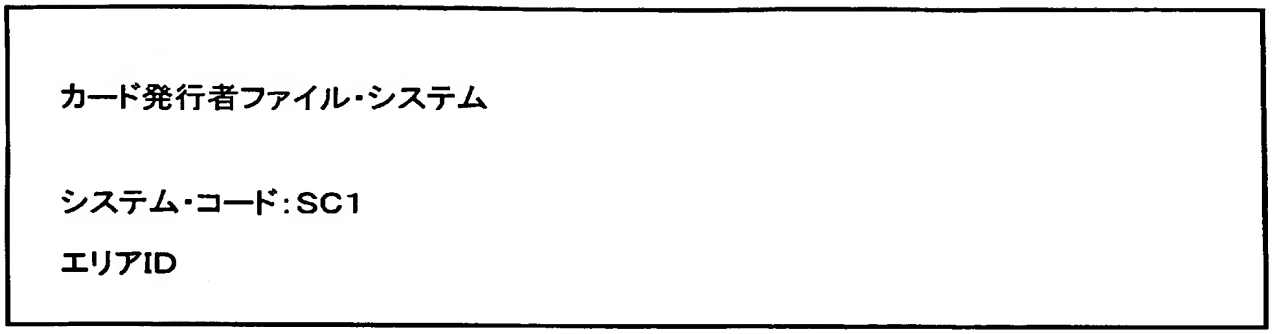
【図１】



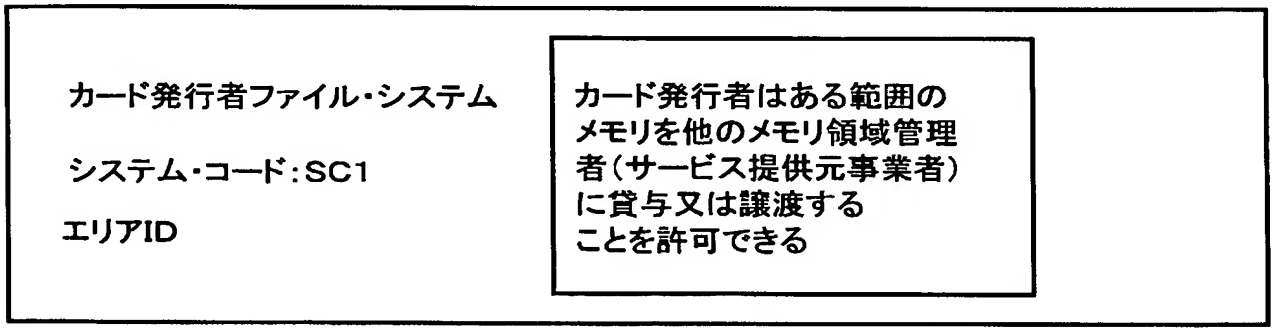
【図２】



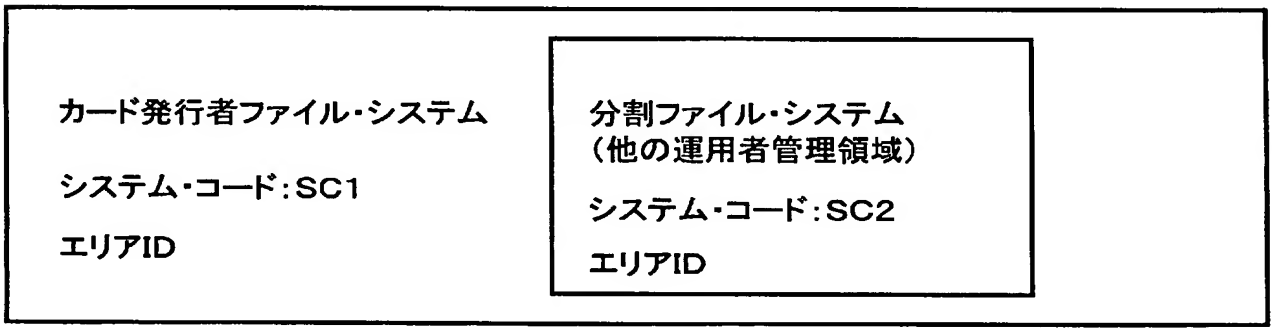
【図３】



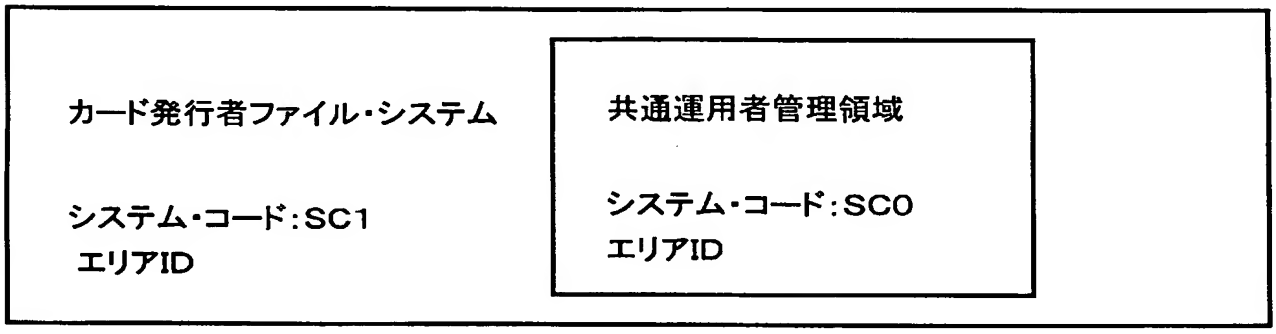
【図４】



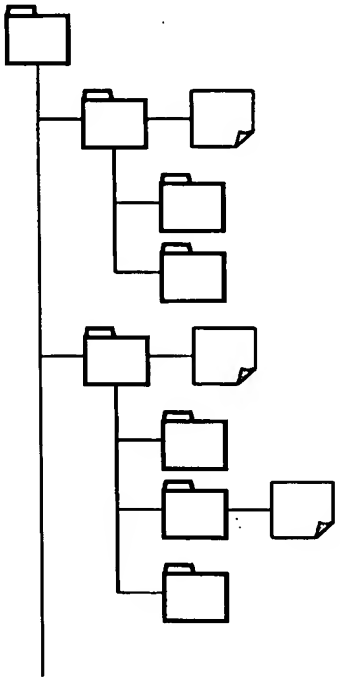
【図５】



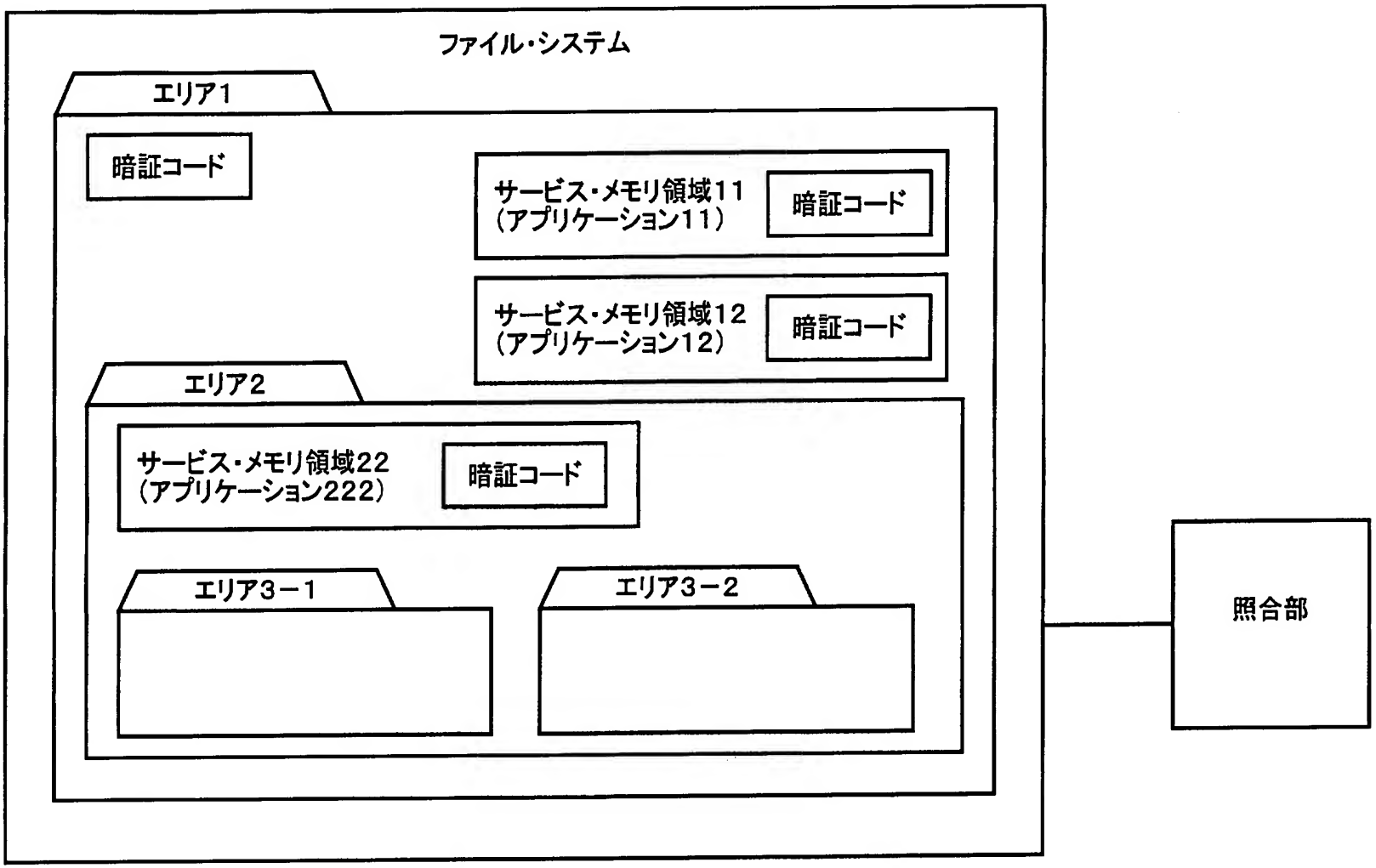
【図６】



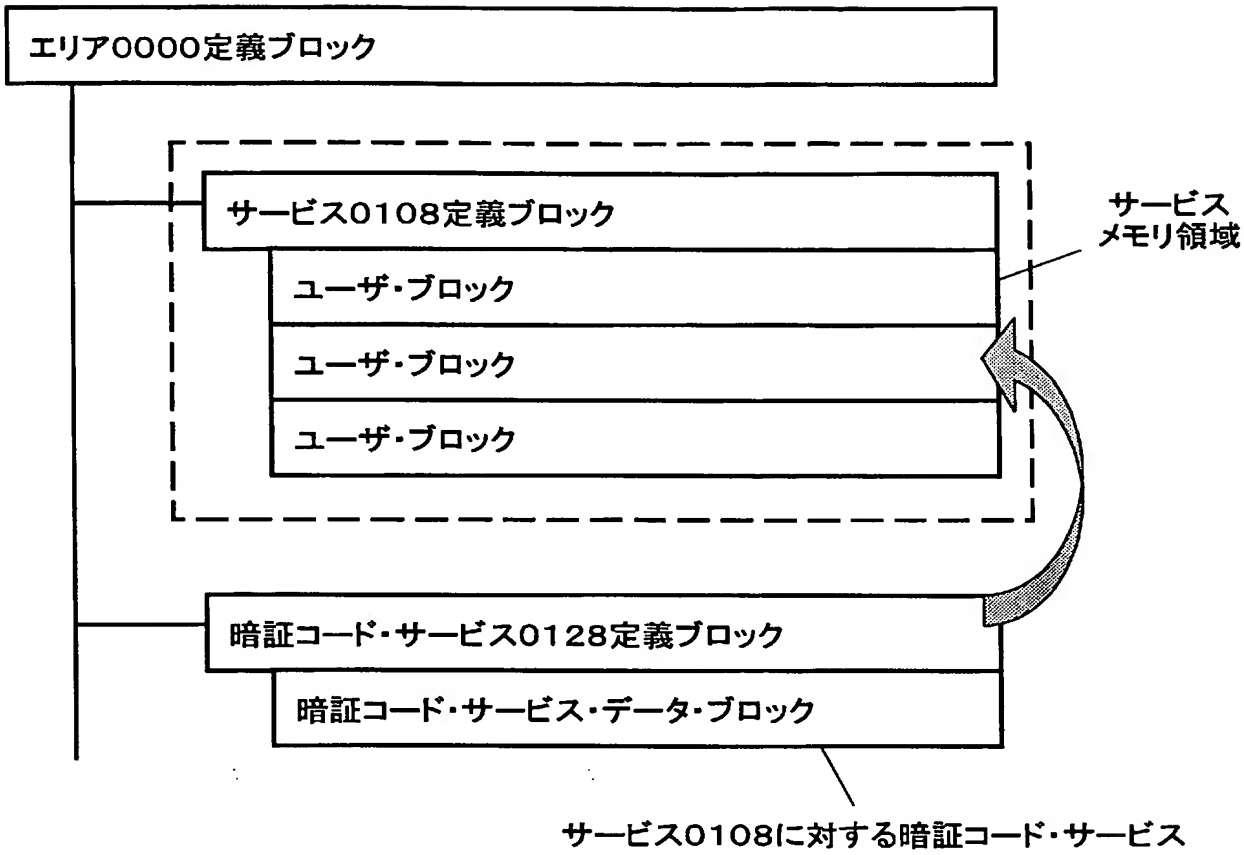
【図７】

ファイル・システム#0	#1	#1	#1
システム・コードSD#0	SD#1	SD#1	SD#1
エリアID#0	ID#1	ID#1	ID#1
			

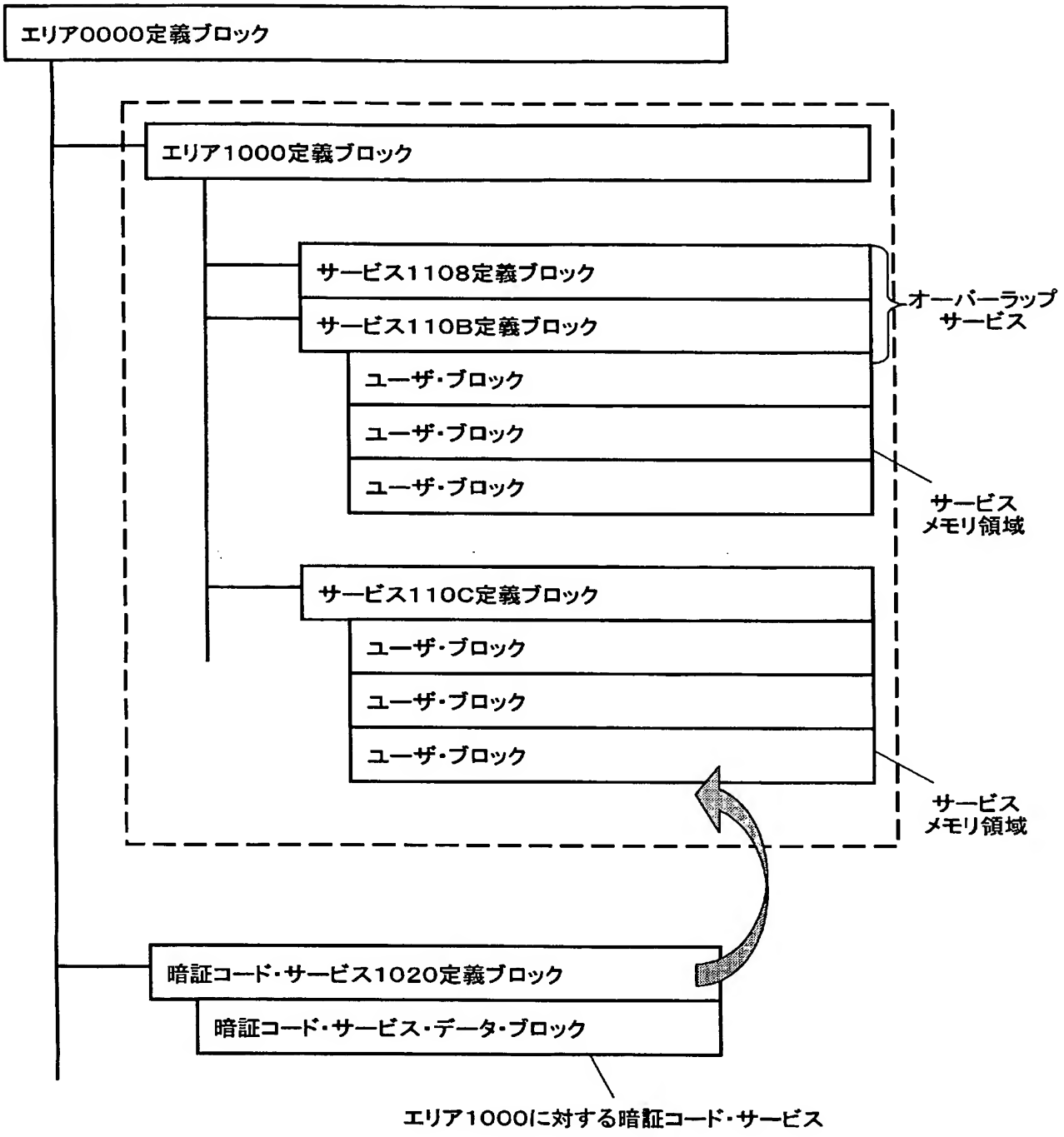
.....

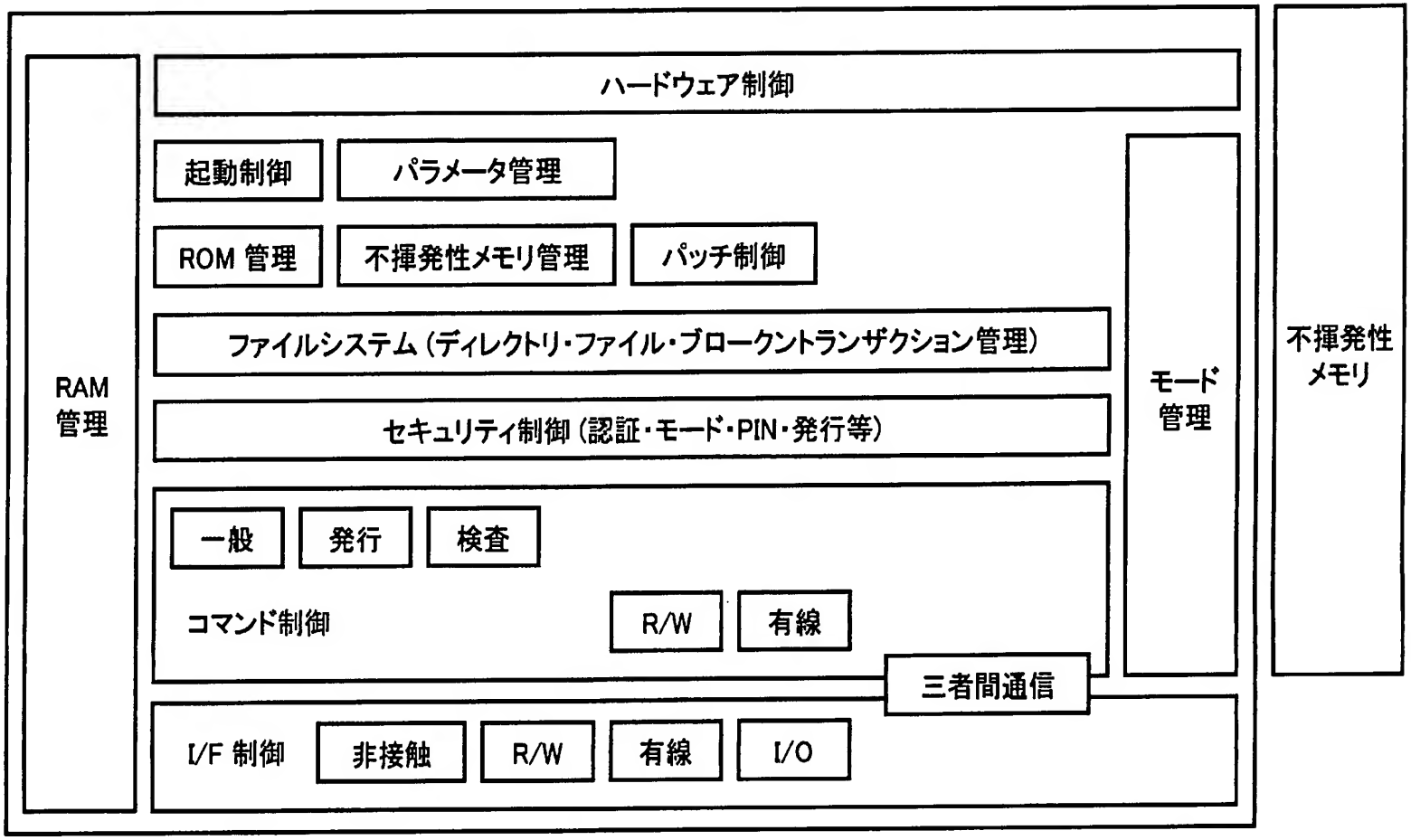

ファイル・システム
エリア1
暗証コード
サービス・メモリ領域11
(アプリケーション11)
暗証コード
サービス・メモリ領域12
(アプリケーション12)
暗証コード
エリア2
サービス・メモリ領域22
(アプリケーション222)
暗証コード
エリア3－1
エリア3－2
照合部

【図９】

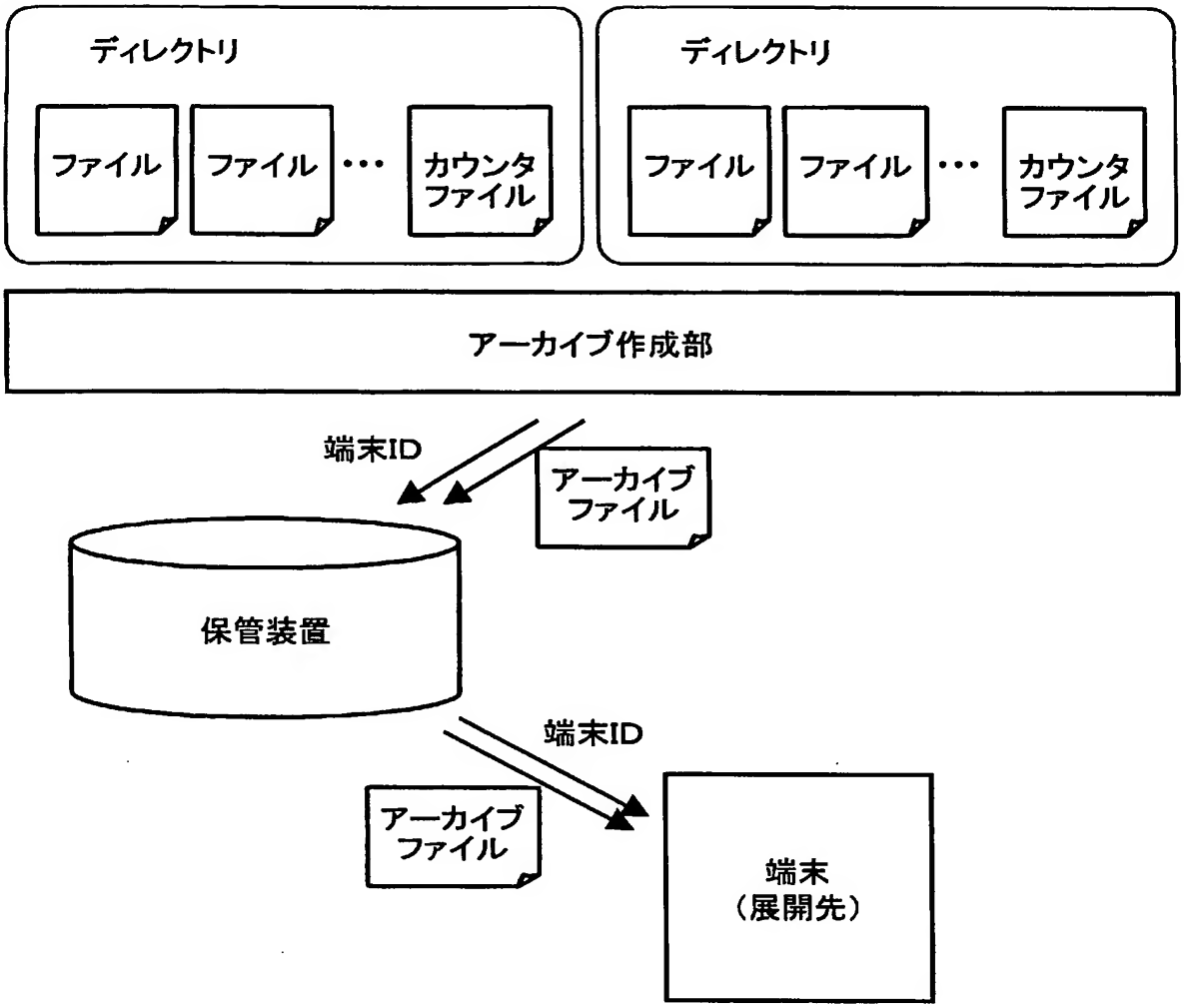

エリア0000定義ブロック
サービス0108定義ブロック
ユーザ・ブロック
ユーザ・ブロック
ユーザ・ブロック
サービス
メモリ領域
暗証コード・サービス0128定義ブロック
暗証コード・サービス・データ・ブロック
サービス0108に対する暗証コード・サービス

【図１０】

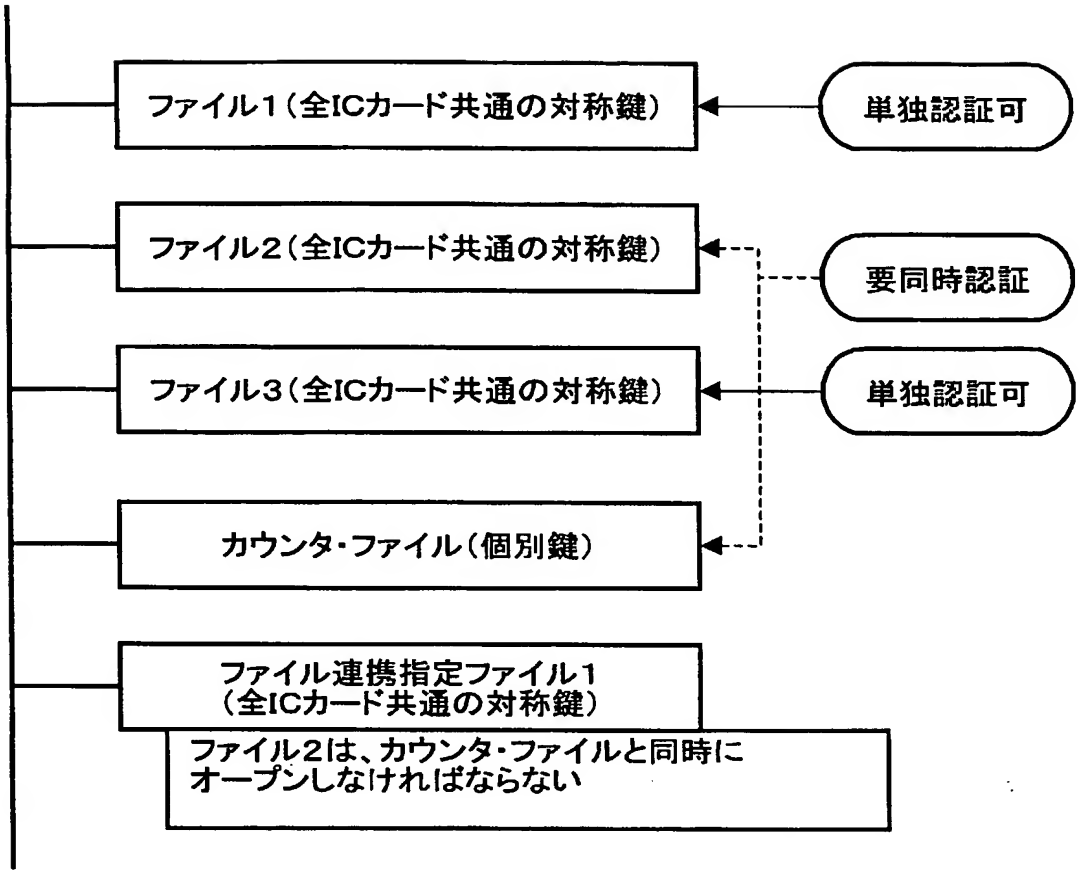

エリア0000定義ブロック
エリア1000定義ブロック
サービス1108定義ブロック
サービス110B定義ブロック
オーバーラップ
サービス
ユーザ・ブロック
ユーザ・ブロック
ユーザ・ブロック
サービス
メモリ領域
サービス110C定義ブロック
ユーザ・ブロック
ユーザ・ブロック
ユーザ・ブロック
サービス
メモリ領域
暗証コード・サービス1020定義ブロック
暗証コード・サービス・データ・ブロック
エリア1000に対する暗証コード・サービス


RAM
管理
ハードウェア制御
起動制御
パラメータ管理
ROM 管理
不揮発性メモリ管理
パッチ制御
ファイルシステム（ディレクトリ・ファイル・ブロークントランザクション管理）
セキュリティ制御（認証・モード・PIN・発行等）
一般
発行
検査
コマンド制御
R/W
有線
三者間通信
I/F 制御
非接触
R/W
有線
I/O
モード
管理
不揮発性
メモリ

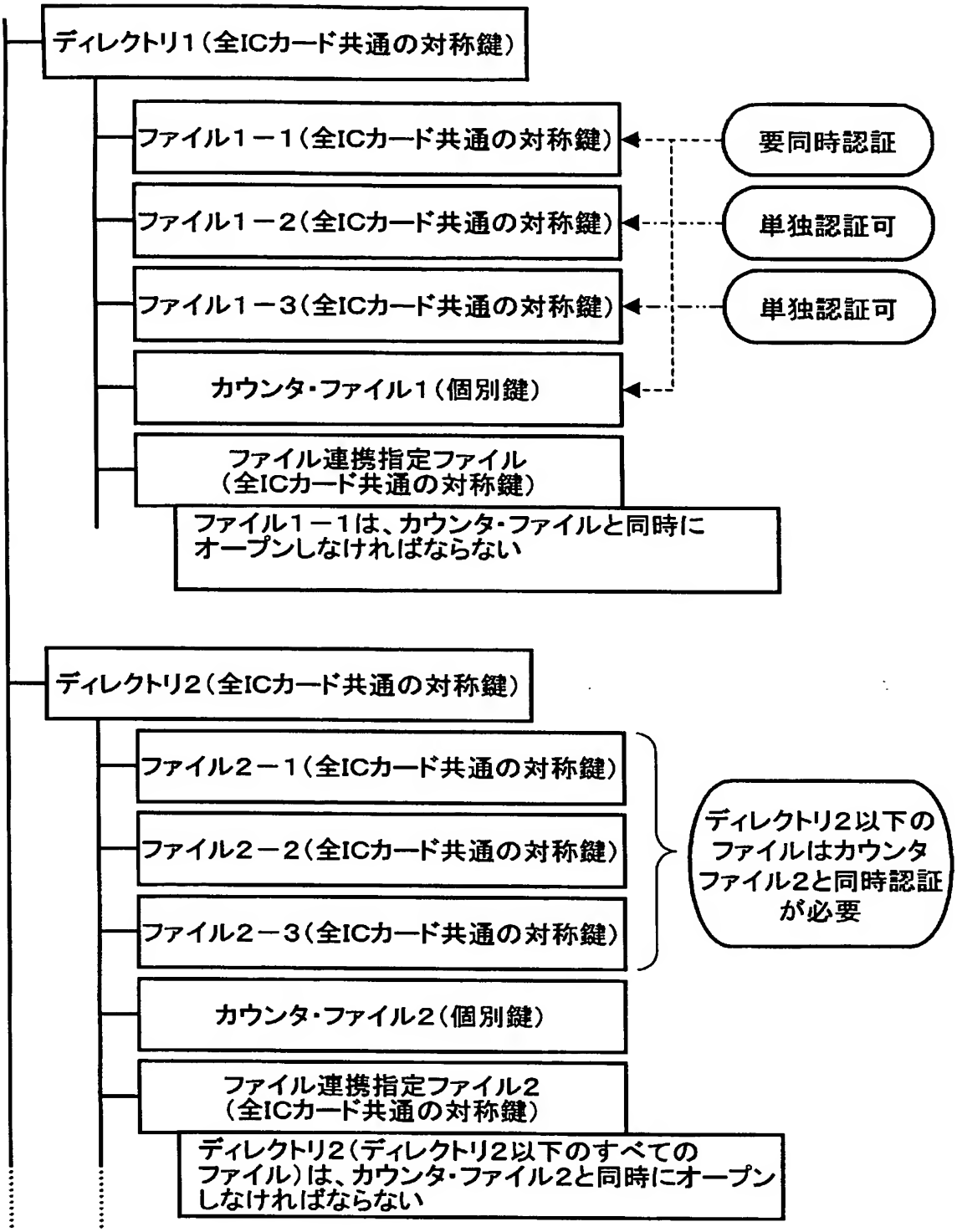
【図１２】


ディレクトリ
ファイル
ファイル
カウンタファイル
ディレクトリ
ファイル
ファイル
カウンタファイル
アーカイブ作成部
端末ID
アーカイブファイル
保管装置
端末ID
アーカイブファイル
端末
（展開先）

【図１３】


ファイル1（全ICカード共通の対称鍵）
単独認証可
ファイル2（全ICカード共通の対称鍵）
要同時認証
ファイル3（全ICカード共通の対称鍵）
単独認証可
カウンタ・ファイル（個別鍵）
ファイル連携指定ファイル1
（全ICカード共通の対称鍵）
ファイル2は、カウンタ・ファイルと同時に
オープンしなければならない

【図１４】


ディレクトリ1（全ICカード共通の対称鍵）
ファイル１－１（全ICカード共通の対称鍵）
ファイル１－２（全ICカード共通の対称鍵）
ファイル１－３（全ICカード共通の対称鍵）
カウンタ・ファイル１（個別鍵）
ファイル連携指定ファイル
（全ICカード共通の対称鍵）
ファイル１－１は、カウンタ・ファイルと同時に
オープンしなければならない
要同時認証
単独認証可
単独認証可
ディレクトリ2（全ICカード共通の対称鍵）
ファイル２－１（全ICカード共通の対称鍵）
ファイル２－２（全ICカード共通の対称鍵）
ファイル２－３（全ICカード共通の対称鍵）
カウンタ・ファイル２（個別鍵）
ファイル連携指定ファイル2
（全ICカード共通の対称鍵）
ディレクトリ2（ディレクトリ2以下のすべての
ファイル）は、カウンタ・ファイル2と同時にオープン
しなければならない
ディレクトリ2以下の
ファイルはカウンタ
ファイル2と同時認証
が必要

【書類名】 要約書

【要約】

【課題】　メモリ領域上に電子的に格納されている価値情報のコピー若しくはバックアップを行ない、端末間での価値情報の移動を円滑に行なう。

【解決手段】　ＩＣカード内のデータから移動先の端末ＩＤを含めたアーカイブ・ファイルを作成し、所定の保管場所に保管し、価値情報を安全にバックアップする。また、アーカイブ・ファイルは、端末ＩＤで指定された機器でしか展開できないようにする。また、ＩＣカード内のファイルやディレクトリへのアクセスをカウンタで管理する仕組みを導入し、アーカイブ・ファイルを保管場所にアーカイブした後は元のファイルのカウンタ値を消滅させる。

【選択図】　図１２

０００００２１８５
19900830
新規登録
５９７０６２９９３

東京都品川区北品川６丁目７番３５号
ソニー株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/010599

International filing date: 09 June 2005 (09.06.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-175524
Filing date: 14 June 2004 (14.06.2004)

Date of receipt at the International Bureau: 22 July 2005 (22.07.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)